Zuobin Xiong

Assistant Professor · Department of Computer Science

University of Nevada-Las Vegas, 4505 S. Maryland Pkwy. Las Vegas, NV 89154

(702)-895-5897 | zuobin.xiong@unlv.edu | https://zuobinxiong.github.io

Education

Georgia State University — Atlanta, USA

Ph.D., Computer Science — 2018 - 2023

- Advisor: Dr. Wei Li & Dr. Zhipeng Cai

Harbin Engineering University — Harbin, China

M.E., Computer Science & Technology — 2016 - 2019

- Advisor: Dr. Qilong Han

Northeast Forestry University — Harbin, China

B.S., Mathematics & Applied Mathematics — 2012 - 2016

- Thesis mentor: Dr. Chunrui Zhang

Professional Experience

2023 - now	**Assistant Professor** Department of Computer Science, University of Nevada-Las Vegas, Las Vegas, NV
2019 - 2023	**Graduate Teaching Assistant** Department of Computer Science, Georgia State University, Atlanta, GA
2018 - 2023	**Graduate Research Assistant** Department of Computer Science, Georgia State University, Atlanta, GA
2016 - 2019	**Graduate Research Assistant** College of Computer Science & Technology, Harbin Engineering University, Harbin, China

Research Interests

I am interested in a broad research area of Data Privacy, ML/AI, Cybersecurity, and IoT

- Private Machine Learning
- Adversarial Machine Learning
- Differential Privacy
- Privacy Inference Attacks
- Intrusion/Anomaly Detection
- Cybersecurity Research/Education
- the Internet of Things
- Distributed Learning

Awards & Honors

Apr. 2023	**Outstanding Graduate Student Award** Awarded by the College of Arts & Sciences, Georgia State University
Feb. 2023	**Student Travel Scholarship** Awarded by AAAI -23 and the Association for the Advancement of Artificial Intelligence
Aug. 2022	**Best Paper Award** Awarded by the 8th IEEE International Conference on Smart Data (SmartData 2022)

Apr. 2021	**Outstanding Graduate Research Award** Awarded by the Department of Computer Science, Georgia State University
2016 - 2018	**First Class Graduate Scholarship Award** Awarded by the College of Computer Science & Technology, Harbin Engineering University

Teaching Experience

Teaching at University of Nevada, Las Vegas

Fall 2023	**CS 789, Advanced Network Security, SEI (TBD)** Instructor, Graduate Level Course, Class Enrollment 10

Teaching at Georgia State University

Spring 2021	**CSC 4222/6222, Intro to Cyber Security, SEI (4.5/5.0)** Instructor, Undergraduate Level Course, Class Enrollment 55
Fall 2019	**CSC 4520/6520, Design and Analysis of Algorithms, SEI (4.7/5.0)** Instructor, Undergraduate Level Course, Class Enrollment 57
Fall 2022	**CSC 4221/6221, Mobile Computing & Wireless Networks** Teaching Assistant
Spring 2022	**CSC 8920, Private and Secure AI (Online)** Teaching Assistant
Fall 2021	**CSC 4520/6520, Design and Analysis of Algorithms** Teaching Assistant
Fall 2020	**CSC 4222/6222, Cyber Security** Teaching Assistant
Spring 2020	**CSC 4740/6740, Data Mining** Teaching Assistant
Spring 2019	**CSC 4740/6740, Data Mining** Teaching Assistant

Research Grants

2021 - 2024	**EDU: Collaborative: Advancing Cybersecurity Learning Through Inquiry-based Laboratories on a Container-based Virtualization Platform** SaTC of NSF, Writing thrusts for my advisor

Publications

Selected Journal Articles

1.	HCC 2023	DEFEAT: A decentralized federated learning against gradient attacks Guangxi Lu, **Zuobin Xiong**, Ruinian Li, Nael Mohammad, Yingshu Li, and Wei Li. *High-Confidence Computing, Volume 3, Issue 3, September 2023.* **(IF: 5.42)**
2.	WWW 2023	Personalized Sampling Graph Collection with Local Differential Privacy for Link Prediction Linyu Jiang, Yukun Yan, Zhihong Tian, **Zuobin Xiong** and Qilong Han. *World Wide Web.* **(IF: 3.000)**
3.	TDSC 2022	Towards Neural Network-based Communication System: Attack and Defense **Zuobin Xiong**, Zhipeng Cai, Chunqiang Hu, Daniel Takabi, and Wei Li. *IEEE Transactions on Dependable and Secure Computing.* **(IF: 6.791)**
4.	CSUR 2022	Generative Adversarial Networks: A Survey Toward Private and Secure Applications Zhipeng Cai, **Zuobin Xiong**, Honghui Xu, Peng Wang, Wei Li, and Yi Pan. *ACM Computing Surveys, Vol. 54, No. 6, Jul. 2022.* **(IF: 10.238)**

5. TII 2022
Privacy Threat and Defense for Federated Learning with Non-iid Data in AIoT
Zuobin Xiong, Zhipeng Cai, Daniel Takabi, and Wei Li. *IEEE Transactions on Industrial Informatics, Vol. 18, No. 2, Feb. 2022.* **(IF: 11.648)**

6. IoT-J 2022
Top-k Socially Constrained Spatial Keyword Search in Large SIoT Networks
Jinbao Wang, **Zuobin Xiong**, Qilong Han, Xixian Han, and Donghua Yang. *IEEE Internet of Things Journal, Vol. 9, No. 12, Jun. 2022.* **(IF: 10.238)**

7. AdHoc 2021
Gated Recurrent Unit-based Parallel Network Traffic Anomaly Detection using Subagging Ensembles
Xiaoling Tao, Yang Peng, Feng Zhao, Changsong Yang, Baohua Qiang, Yufeng Wang, and **Zuobin Xiong**. *Ad Hoc Networks, Vol. 116, 2021.* **(IF: 4.816)**

8. TVT 2021
Multi-Source Adversarial Sample Attack on Autonomous Vehicles
Zuobin Xiong, Honghui Xu, Wei Li, and Zhipeng Cai. *IEEE Transactions on Vehicular Technology, Vol. 70, No. 3, Mar. 2021.* **(IF: 6.239)**

9. TII 2021
ADGAN: Protect Your Location Privacy in Camera Data of Auto-Driving Vehicles
Zuobin Xiong, Zhipeng Cai, Qilong Han, Arwa Alrawais, and Wei Li. *IEEE Transactions on Industrial Informatics, Vol. 17, No. 9, Sept. 2021.* **(IF: 11.648)**

10. WCMC 2021
CGPP-POI: A Recommendation Model Based on Privacy Protection
Gesu Li, Guisheng Yin, **Zuobin Xiong**, and Fukun Chen. *Wireless Communications and Mobile Computing, Vol. 2021, Aug. 2021.* **(IF: 2.146)**

11. SCN 2021
Research on Trajectory Data Releasing Method via Differential Privacy Based on Spatial Partition
Qilong Han, **Zuobin Xiong**, and Kejia Zhang. *Security and Communication Networks, Vol. 2018, Nov. 2018.* **(IF: 1.968)**

Selected Conference Papers

1. ICDM 2023
Exact-Fun: An Exact and Efficient Federated Unlearning Approach
Zuobin Xiong, Wei Li, Yingshu Li, and Zhipeng Cai. *IEEE International Conference on Data Mining.* **(AR: 19.3%)**

2. ICDM 2023
Backdoor Attack on 3D Grey Image Segmentation
Honghui Xu, Zhipeng Cai, **Zuobin Xiong**, and Wei Li. *IEEE International Conference on Data Mining.* **(AR: 19.3%)**

3. ICANN 2023
Sequence-based Modeling for Temporal Knowledge Graph Link Prediction
Wenqiang Liu, Lijie Li, **Zuobin Xiong**, and Ye Wang. *32nd International Conference on Artificial Neural Networks.*

4. AAAI 2023
Federated Generative Model on Multi-Source Heterogeneous Data in IoT
Zuobin Xiong, Wei Li, and Zhipeng Cai. *AAAI Conference on Artificial Intelligence, Washington, DC, USA, Feb. 2023.* **(AR: 19.6%)**

5. Globecom 2022
Pairwise Gaussian Graph Convolutional Networks: Defense Against Graph Adversarial Attack
Guangxi Lu, **Zuobin Xiong**, Jing Meng, and Wei Li. *IEEE Global Communications Conference, Rio de Janeiro, Brazil, Dec. 2022.*

6. WiCON 2022
Decentralized Federated Learning: A Defense against Gradient Inversion Attack
Guangxi Lu, **Zuobin Xiong**, and Wei Li. *EAI International Conference on Wireless Internet, Dallas, USA, Nov. 2022.*

7. SmartData 2022
A Self-Supervised Purification Mechanism for Adversarial Samples
Bingyi Xie, Honghui Xu, **Zuobin Xiong**, Yingshu Li, and Zhipeng Cai. *IEEE International Conference on Smart Data, Espoo, Finland, Aug. 2022. (Best Paper Award).*

8. SEKE 2022
Exp-SoftLexicon Lattice Model Integrating Radical-Level Features for Chinese NER
Lijie Li, Shuangyang Hu, Junhao Chen, YeWang, and **Zuobin Xiong**. *International Conference on Software Engineering & Knowledge Engineering, Pittsburgh, USA, Jul. 2022.*

9. ICDM 2019
Privacy-Preserving Auto-Driving: a GAN-based Approach to Protect Vehicular Camera Data
Zuobin Xiong, Wei Li, Qilong Han, and Zhipeng Cai. *IEEE International Conference on Data Mining (ICDM), Beijing, China, Nov. 2019.* **(AR: 9.08%)**

Presentations

Invited Talks

Nov. 2022	**On the Privacy Inference and Protection of Federated Learning** College of Computer Science and Technology, Harbin Engineering University
Spet. 2022	**Towards Privacy Preservation of Federated Learning in Artificial Intelligence of Things** Department of Electrical and Computer Engineering, Virginia Commonwealth University
Aug. 2022	**Privacy Threats and Defense in Federated Learning** Department of Computer Science, University of Electronic Science and Technology of China

Professional Services

Academic Membership

- Member of IEEE
- Member of AAAI

PC Member

- 32nd International Conference on Artificial Neural Networks (ICANN)

Editorship

- Guest Editor – MDPI Electronics

Conference Reviewer

- IEEE Global Communications Conference (GLOBECOM)
- IEEE Cyber Science and Technology Congress
- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)

Journal Reviewer

- ACM Transactions on Sensor Networks (TOSN)
- Discrete Mathematics, Algorithms and Applications (DMAA)
- IEEE Transactions on Industrial Informatics (TII)
- IEEE Transactions on Vehicular Technology (TVT)
- IEEE Internet of Things Journal (IoT-J)
- IEEE Transactions on Wireless Communications (TWC)
- IEEE Transactions on Knowledge and Data Engineering (TKDE)
- IEEE Transactions on Network Science and Engineering (TNSE)
- IEEE Transactions on Computational Social Systems (TCSS)
- Elsevier Neurocomputing
- Elsevier Computer & Security
- Elsevier Computer Communications
- Elsevier High-Confidence Computing
- Security and Communication Networks
- Springer Scientific Reports - Nature
- Springer Artificial Intelligence Review
- Springer Journal of Big Data